UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT: 1109 Tremont St, Poplar Bluff, MO 63901 located in the Eastern District of Missouri.	)))))	No. 1:22MJ4218 ACL FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

In re search of:

SEE ATTACHMENT A

I, Thomas Putting, a Special Agent with Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1109 Tremont St, Poplar Bluff, MO 63901 which is located in the Eastern District of Missouri (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent ("SA") of the U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations ("HSI"), since March 2019, and I am currently assigned to the HSI office in Saint Louis, Missouri. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) in Brunswick, Georgia, and everyday work relating to conducting these types of investigations. I

have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 1470, 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1) and (2) (distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography) (hereinafter the "SUBJECT OFFENSES") are presently located at the location to be searched, and within computer(s) and related peripherals, computer hardware and media, and wireless telephones found at that location.

LOCATION TO BE SEARCHED

5. The location to be searched is 1109 Tremont Street, Poplar Bluff, MO 63901 located in the Eastern District of Missouri (the "SUBJECT PREMISES"), which is a two-story single-family residence with white siding and brick. The garage appears to be on the bottom floor of the residence. There is "1109" in black numbering to the right of the front door. Also to be searched is a white Ford Focus bearing Missouri License plate ED2 B1G that is registered to the occupant of 1109 Tremont Street, Poplar Bluff, namely, Joseph Fleming. A photograph of the home and vehicle is attached to this Affidavit and included in "Attachment A".

STAUTORY AUTHORITY

6. The investigation concerns the alleged violations of Title 18, United States Code, Sections 2251 and 2252, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and federal prosecutors, I know the following:

a. 18 U.S.C. § 2251(a) in pertinent part prohibits a person from using, persuading, inducing, enticing, or coercing any minor to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if that visual depiction was produced using any means or facility of interstate commerce, to include, by computer.

b. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with the intent to view any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate commerce, that is, by computer or mails.

c. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. 2256(8), using any means or facility of interstate of foreign commerce or in or affecting interstate or foreign commerce, including by computer.

d. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or affecting interstate or foreign commerce, including by computer or mails, any visual

depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate of foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate commerce or through the mails. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to knowingly possess or knowingly access with intent to view, one or more books, magazines, periodicals, films or other materials which contain visual depictions of minors engaged in sexually explicit conduct that has been mailed or has been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped, or transported by any means including by computer.

e. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing, or knowingly accessing

with the intent to view, any material that contains an image of child pornography that has been shipped, mailed, or transported using any means or facility of interstate commerce, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. Sections 2252 and 2256(2).

c. "Visual depictions," include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between two persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or ports that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work.

Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDSs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Computer passwords and data security devices," as used herein, consists of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different number to a computer every time it accesses the Internet. IP addresses might also be static, meaning that the ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of www.usdoj.gov may refer to an IP address of "149.101.1.32." Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

l. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. A "Preservation Letter" is a letter that a government entity may issue to internet service providers pursuant to Title 18, United States Code, Section 2703(f), to ensure that the internet service providers preserve records in their possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted.

n. "Internet Service Providers" or "ISPs," as used herein, are commercial organizations that provide individuals and businesses access to the internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communication equipment.

ISPs can offer various means by which to access the Internet, including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an email address, and an email mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

o. "Cloud storage" is an online central storage location, which allows users to access their files from anywhere using a device connected to the Internet.

p. "Wireless telephone," "mobile telephone," or "cellular telephone," as used herein, means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing data, appointments, and other information on personal calendars; and accessing and

downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

CHILD PORNOGRAPHY COLLECTOR CHARATERISTICS

8. Based on my training, experience and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect child pornography. I have observed and learned about the reliability of these commonalities and conclusions involving individuals, who collect, produce and trade images of child pornography. I know the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means to gaining status, trust, acceptance and

support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P), e-mail, e-mail groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium form which they were derived, in telephone books or notebooks, on the computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other likeminded individuals over the Internet. As such, they tend to maintain or "hoard" their visual

depictions of child pornography for long periods of time in the privacy and security of their homes and other secure locations. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on moveable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted or send it to third party image storage sites via the Internet.

BACKGROUND ON KIK

9. Kik advertises itself as "the first smartphone messenger with a built-in browser". KIK Messenger allows its users to "talk to your friends and browse and share any web site with your friends on KIK." KIK believes it is at the forefront of the "new era of the mobile web." KIK was founded in 2009 by a group of University of Waterloo students who started a company designed to "shift the center of computing from the PC to the phone." According to the website, KIK Messenger, a free service easily downloaded from the Internet, KIK has become the simplest, fastest, and most life-like chat experience you can get on a smartphone. Unlike other messengers, KIK uses names, "usernames," not phone numbers, as the basis for KIK user accounts, so KIK users are in complete control with whom they communicate. In addition, KIK features include more than instant messaging. KIK users can exchange images, videos, sketches, stickers and even more with mobile web pages.

10. The KIK app is available for download via the App Store for most iOS devices such as iPhones and iPads. Additionally, the KIK app is available on the Google PlayStore for Android devices. KIK can be used on multiple mobile devices, to include cellular phones and tablets.

11. In general, providers like KIK ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address.

12. Providers typically retain certain transaction information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can hep to identify which computers or other devices were used to access the account.

13. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems or complaints from other users. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider's support

services, as well as records of any actions taken by the provider or user as a result of the communications.

14. KIK offers users the ability to create an identity within the app referred to as a "username". This username is unique to the account and cannot be changed. No one else can utilize the same username. A KIK user would have to create a new account in order to obtain a different username. The username for a particular KIK account holder is displayed in their KIK profile.

15. In October 2019, KIK was purchased by MediaLab, a company operating in the United States.

PROBABLE CAUSE

16. On or about May 31, 2022, your affiant was notified of a Kik Report forward from Kik/MediaLab (Kik) to the National Center for Missing and Exploited Children (NCMEC), which was then forwarded to the Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) (referred to as, C3-CEIU). This Kik report included copies of suspected child pornography which was reviewed by your affiant. These images had previously been located, isolated, searched, and viewed by Kik personnel before they were reported to NCMEC. Your affiant reviewed only the images previously located, isolated, searched and viewed by Kik personnel and observed that the images are of child pornography as defined by Federal Law.

17. Your affiant reviewed a NCMEC CyberTip Report (CT # 123586249) dated April 29, 2022. A review of the report showed that between March 16, 2022 and April 11, 2022, Kik user, who provided the name Joseph Fleming, a username of "worldchampz1", and an email address of flemingjoseph95@gmail.com, used Kik to upload approximately 169 files of child

pornography. Additionally, the report listed the device used to register this account as a Samsung Android phone.

18. On or about July 20, 2022, your affiant reviewed the images of child pornography that was contained within the report, which was provided to HSI by Kik. Out of the 169 files, approximately 123 were of child pornography. This not to say that the other forty-six (46) video files were not child pornography but they were too age difficult to determine. Below is a description of two of the video files as an example of what was depicted:

a. "0c40f5ad-6c02-4dd2-af5f-c849ca50db74" is a video file approximately one (1) minute and twenty-four (24) seconds in length, that depicts, in part, a minor prepubescent female, approximately eight (8) to nine (9) years of age, rubbing her vagina with her hands. The prepubescent minor female is wearing a pink shirt and has pink shorts pulled down to her ankles. There appears to be an apparent adult male's hand that appears on camera and rubs the prepubescent minor female's thighs. The prepubescent minor female then takes her shorts off completely and then starts to insert her finger into her vagina at what appears to be by direction of someone off screen.

b. "0d404489-02b6-44b7-b487-fcf6c05809af" is a video file approximately one (1) minute and one (1) second in length, that depicts, in part, an apparent adult male inserting his penis into the anus of a nude prepubescent minor female who is approximately five (5) to six (6) years of age.

19. On or about June 2, 2022, your affiant served ICE Administrative Summons (ICE-HSI-SU-2022-004673) to Sparklight, for subscriber information on IP address 108.175.248.83, used on March 16, 2022 at 01:22:49 UTC and 11:38:38 UTC, and on April 6,

2022 at 19:54:56 UTC. On or about June 3, 2022, Sparklight responded with the following subscriber information.

Name:	Gina Kasal
Service Address:	1109 Tremont St, Poplar Bluff, MO 63901
Mailing Address:	1109 Tremont St, Poplar Bluff, MO 63901
Phone:	573-208-9930
Account No:	130312127
Email Address:	gkasa188@gmail.com
Customer Status:	Active
Creation Date:	02/21/2020
IP Address:	108.175.248.83
MAC Address:	68:8f:2e:70:84:83
Lease Start Date:	03/14/2022
Lease End Date:	04/11/2022

20. On or about June 2, 2022, your affiant served ICE Administrative Summons (ICE-HSI-SU-2022-004665) to Google, Inc, requesting the basic subscriber information and IP log for the following email address flemingjoseph95@gmail.com. On June 2, 2022, a response was received from Google, Inc, which provided the following information:

Google Account ID:	635135526764
Name:	Joseph FLEMING
Email:	flemingjoseph95@gmail.com
Created on:	07/15/2018
Terms of Service IP:	75.132.245.38

Last Updated Date:	06/01/2022
Recover Email:	capetigers2014@gmail.com
Recover SMS:	573-772-1530

Google, Inc, also provided Google Pay information as follows:

Payments Profile ID:	9453-2210-1179
Contact Email:	flemingjoseph95@gmail.com
Payment Profile Creation:	09/26/2019 04:12:34 UTC
Billing Address:	3028 Themis St, Apt C, Cape Girardeau, MO 63701
Billing Name:	Joseph A. Fleming
Billing Name:	Gina Kasal

On 08/10/2021 a credit card was added to the Google pay account with the billing name of Gina Kasal.

21. On August 12, 2022, your affiant queried a public database system. The query revealed that a Gina Kasal with a date of birth of XX XX 1981, and a Joseph A. FLEMING with a date of birth of XX XX 1995 reside at 1109 Tremont St, Poplar Bluff, MO 63901.

22. On August 11, 2022, a Poplar Bluff City Police Department (PBCPD) Officer conducted surveillance of the SUBJECT PREMISES and observed a white Ford Focus bearing Missouri license plate "ED2 B1G". A check with a government database system revealed the vehicle was registered to Joseph FLEMING with a registered address of the SUBJECT PREMISES.

23. On August 17, 2022, your affiant conducted surveillance at the SUBJECT PREMISES and observed the white Ford Focus bearing Missouri license plate "ED2 B1G" along

with an Orange Jeep bearing Missouri license plate "EB4 L5E". A check with a government database system revealed the Orange Jeep vehicle was registered to Gina Kasal.

24. On August 17, 2022, your affiant used his government-issued iPhone in an effort to gain additional information regarding any potential wireless networks at the SUBJECT PREMISES. Positioned approximately five (5) yards from the SUBJECT PREMISES, your affiant noted that there were multiple wireless networks in the area, but all of them were secured. Accordingly, to use any of them to access the Internet, a user would likely have to know the encryption key or password for that particular network. Based on the signal strength of the wireless networks, as well as my training and experience and information relayed to me by agents, your affiant believes that the wireless router at the SUBJECT PREMISES is likely generating a secured wireless network. As explained above, I know from my training and experience and information relayed to me by agents, that wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime.

25. On August 22, 2022, your affiant contacted a representative of Poplar Bluff Municipal Utilities to request information on who is responsible for the utilities at the SUBJECT PREMISES. The representative informed your affiant that a Gina Kasal and Joseph FLEMING currently have services at the SUBJECT PREMISES since March of 2021.

PAST KIK LEAD ON JOSEPH FLEMING

26. In December 2019, Homeland Security Investigations (HSI) St. Louis was notified of a Kik Report forward from Kik to the NCMEC, which was then forward to the C3-CEIU. This was when Kik was still headquartered in Canada. The lead referenced that a Kik user with the username "worldchampz06", a name of Joseph FLEMING, and an email address of

capetigers2014@gmail.com sent and or received an image of child pornography. Kik flagged the image utilizing PhotoDNA and notified NCMEC of the user. HSI St. Louis was able to identify Kik user "worldchampz06" as FLEMING. Because of COVID-19 a knock and talk was never conducted.

SEIZURE OF EQUIPMENT AND DATA

27. Based upon my knowledge, training and experience, I know that in order to completely and accurately retrieve data maintained in computer hardware, including cellular telephones, or on computer software, to ensure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process may take weeks or months, depending on the volume of data stored and it would be impractical to attempt this kind of data analysis on-site.

b. Technical requirements. Analyzing computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled

environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

28. Due to the volume of the data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such-- or whether is serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readable, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be

analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

29. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

30. Based upon my knowledge, training, and experience, and the experience of other law enforcement personnel with whom I have spoken, I am aware that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize

most or all of a computer system's input/output peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPU) and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

31. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access

the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

COMPUTER EXAMINATION METHODOLOGY TO BE EMPLOYED

32. The examination procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other examination procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC ACCESS

33. Many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

34. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

35. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. Apple's facial recognition feature is referred to as Face ID and it allows a user to unlock the iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user's face. Face ID confirms attention by detecting the

direction of the user's gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user's appearance, and carefully safeguards the privacy and security of the user's biometric data. Similarly, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

36. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

37. Beginning with the release of Apple's iOS 8 operating system in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device.

38. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

39. As discussed in this Affidavit, there is reason to believe that one or more digital electronic devices, (Device(s)), will be found during the search. The passcode or password that would unlock any Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

40. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Further, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law

enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

41. A person who is in possession of a Device or has the Device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometric data, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

CONCLUSION

42. Based on the above information, there is probable cause to believe that the SUBJECT OFFENSES have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES described in Attachment A, and any computers, computer media, or wireless telephones therein, and more fully described herein. Your Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for these premises and all computers, computer hardware and media, and wireless telephones therein.

I state under the penalty of perjury that the foregoing is true and correct.

THOMAS PUTTING
Special Agent
Homeland Security Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on September 29 **, 2022.**

Abbie Crites-Leoni

HONORABLE ABBIE CRITES-LEONI
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The location to be searched is 1109 Tremont Street, Poplar Bluff, MO 63901 located in the Eastern District of Missouri (the "SUBJECT PREMISES"), which is a two-story single-family residence with white siding and brick. The garage appears to be on the bottom floor of the residence. There is "1109" in black numbering to the right of the front door. Also to be searched, a white Ford Focus bearing Missouri License plate ED2 B1G that is registered to the occupant of 1109 Tremont Street, Poplar Bluff, namely, Joseph Fleming.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

All records, items, and information constituting evidence, instrumentalities and contraband concerning the violations of 18 U.S.C. §§ 2252A(a)(1) (distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), including as follows:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:

   a. Any computer, cell phone, computer system and related peripherals including any data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);

   b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and

   c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.

4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence and the items to be seized including, including any and all records or correspondence, in any format or medium (including but not limited to email messages, chat logs, and other electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including by computer, any child pornography as defined in Title 18, United States code, Section 2256(2)..

5. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.

6. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.

The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person(s) state or otherwise provide the password or any other means that may be used to unlock or access the Device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask the aforementioned person(s) to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s).